EXHIBIT 9

ECFMG™ EDUCATIONAL COMMISSION FOR FOREIGN MEDICAL GRADUATES Policy and Procedures Manual	SUBJECT: *CSEC DATA SECURITY POLICY*	POLICY NO: *237*
	DEPARTMENT: ECFMG CSEC Center Operations	
	DISTRIBUTION: *CSEC*	
	EFFECTIVE DATE: *6/10/2007*	Page 1 of 3

I. POLICY

This policy describes the security procedures that must be followed to safeguard and protect the intellectual property and confidential data of the CSEC with respect to center operations managed and operated by ECFMG. This policy covers all ECFMG CSEC employees and all ECFMG employees who process and work with CSEC data.

Any compromise or misappropriation of USMLE Step 2 CS data will have serious implications for the integrity of the CSEC examination process and the United States Medical Licensing Examination, (USMLE). Accordingly this policy and related procedures shall be strictly enforced.

II. DEFINITIONS

Confidential and Sensitive – "Confidential and Sensitive" material relates to data that is proprietary to ECFMG or USMLE/NBME, and if exposed or divulged would cause significant and lasting harm to the ECFMG/NBME/USMLE CSEC testing program. Without limiting the meaning of the foregoing, "Confidential and Sensitive" applies to all case bank materials, training materials, and all materials used by examinees during the examination. It also includes any personal information about ECFMG Standardized Patient employees who are matched to patient cases such as age, race, gender, etc.

FTP – File Transfer Protocol. FTP is an internet protocol for transferring large data files.

USB – Universal serial bus. A widely used hardware interface for attaching peripheral devices. Typically USB ports are used to transfer data to a portable data storage device such as a "flash" or "thumb" drive.

III. ELIGIBILITY

This policy applies to all CSEC ECFMG employees, both exempt and non-exempt and includes part time as needed employees including standardized patients, proctors, trainers, etc. The policy also covers ECFMG employees that work with and process CSEC data such as IT employees, independent contractors and other individuals that may be employed to work in the CSEC operations area.

IV. PROCEDURES

Encryption of Sensitive and Confidential data

- All DVDs containing test materials/cases shall be compressed, encrypted and password protected.
- All data stored on hard drives or other media that is considered sensitive and confidential shall be encrypted using industry standard encryption software. Users shall only be able to save to a specific designated folder on their local drive. This local designated folder shall be encrypted automatically.

Ellis
EXHIBIT NO. 24
P. Antone, CRR

Access to case materials and other confidential data.

Access to case bank materials shall be limited to "on a need to know" basis. Access rights and privileges shall be granted based upon the duties and responsibilities of the individual. Access to data shall be supplied when the individual logs on to the application and will be managed at the server and application levels. Periodically all individuals with access rights will be reviewed by center operations staff to ascertain that the access levels remain appropriate. Terminated individuals shall be immediately removed from access of any kind in accordance with ECFMG's termination policy.

Physical security of SP laptops

- All laptops used by Standardized patients will be visually accounted for at the end of each examination session by IT end user support and/or trainer on duty. SP laptops shall be cable locked inside the training exam rooms and phone rooms and shall not be removed unless authorized or required by IT support staff and the Center management.
- SP laptops shall not have access to internet sites other than those sites required for the conduct of the examination.
- No SP laptops shall have FTP capability.
- USB ports shall be disabled.
- Doors to the SP training room are to remain locked when not in use during the day and locked at the end of each day.

Physical security of Trainer laptops

- Trainers assigned laptops will securely store the laptops at the center at which they work.
- Central Trainer Specialists will have the occasional need to travel between sites and they should not check the laptops with other baggage or otherwise leave them unattended for any reason but always have the laptops in their presence while traveling.

E-case files on both SP and Trainer laptops

- E-case files are cached in the temp folder of the laptops during browser sessions. Each browser program will be set to delete all cached files upon browser close. This setting shall not be capable of being modified by any user.

Ability to download data from Training Room laptops and Exam Room PCs.

- Training Room laptops and Exam Room PCs shall only be loaded with e-case and the SPDE application.
- Training Room laptops shall not have general internet access or e-mail.
- Exam Room PCs shall have e-mail access only to the ECFMG Exchange server and no internet access shall be provided.
- Laptops shall not be connected to printers or any other device that is capable of transmitting confidential case material.
- USB ports shall be disabled.

Ability to download data from Center Manager, Assistant Manager and Trainer laptops and PCs

- Each manager, assistant manager and trainer shall adhere to ECFMG's current password security policy and shall not share or communicate their password with any other person.
- Trainer laptops shall be loaded with e-case, have video capability, be supplied with the current MS Office application, be provided internet access and e-mail.
- Center Managers, Assistant Managers and Trainers shall be provided print capability for e-case materials.
- ~~Center Managers, Assistant Managers and~~ Trainer laptops shall have their USB port disabled.

Patient Note Raters

- Patient Note Raters (PNRs) shall be supplied access to case summaries, key words/concepts, transient PE findings, for ONLY those cases that they are assigned to rate.
- Storing or printing any files generated by the application on the note rater's local drive is strictly prohibited.
- All offsite rating of patient notes will take place at the note rater's home, which will be defined as the place of residence as designated on ECFMG® personnel records.
- No patient notes may be viewed or scored outside of the home via the browser-based patient note rating application or any other method.
- VPN software may only be installed on one designated personal computer located at the place of residence. Raters who choose to install the VPN software on a personal laptop computer may not view or score notes at their place of employment, while traveling, or at any other time or place outside of the home.
- The VPN password/token must be kept secure at the place of residence.
- Raters may still choose to score notes onsite at the ECFMG office using the Internet-based rating application, in which case the VPN log-on will not be required.
- Patient notes and case materials are confidential materials that are the property of USMLE and may only be accessed online. Patient notes and case materials may not be printed and/or shared with any other person.

Confidentiality Statement

All CSEC ECFMG employees and ECFMG employees who work with sensitive and confidential materials will be required to sign the CSEC Ownership, Confidentiality, and Non-Disclosure Agreement in accordance with CSEC/NBME and ECFMG's confidentiality policy.

Responsibility for Policy: Client Services Manager

Approved by Senior Staff on June 10, 2007
Date

Approved by Human Resources on ______________________________
Date

Approved by President ______________________________**Date June 10, 2007**
James A. Hallock, MD President